ROBBINS GELLER RUDMAN
& DOWD LLP
RACHEL L. JENSEN (211456)
655 West Broadway, Suite 1900
San Diego, CA 92101
Telephone: 619/231-1058
619/231-7423 (fax)
rachelj@rgrdlaw.com
– and –
PAUL J. GELLER
STUART A. DAVIDSON
MARK DEARMAN
120 E. Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
pgeller@rgrdlaw.com
sdavidson@rgrdlaw.com
mdearman@rgrdlaw.com

LABATON SUCHAROW LLP
CHRISTOPHER J. KELLER
HOLLIS L. SALZMAN
KELLIE LERNER
CAROL C. VILLEGAS
140 Broadway
New York, NY 10005
Telephone: 212/907-0700
212/818-0477 (fax)

Attorneys for Plaintiffs

[Additional counsel appear on signature page.]

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

FELIX CORTORREAL, JACQUES DAOUD JR. and JIMMY CORTORREAL, on Behalf of Themselves and All Others Similarly Situated,

Plaintiffs,

vs.

SONY CORPORATION OF AMERICA, INC., SONY COMPUTER ENTERTAINMENT OF AMERICA, LLC, SONY PICTURES ENTERTAINMENT, INC., and SONY NETWORK ENTERTAINMENT INTERNATIONAL, LLC,

Defendants.

Case No. '11CV1369 L NLS

CLASS ACTION

COMPLAINT FOR:

(1) VIOLATIONS OF CAL. CIVIL CODE §1750, *et seq.*;

(2) VIOLATIONS OF CAL. BUS. & PROF. CODE §17200, *et seq.*;

(3) VIOLATIONS OF 18 U.S.C. §2702, *et seq.*;

(4) NEGLIGENCE;

(5) BREACH OF EXPRESS CONTRACT; and

(6) BREACH OF FIDUCIARY DUTY

DEMAND FOR JURY TRIAL

Plaintiffs Felix Cortorreal, Jacques Daoud Jr. and Jimmy Cortorreal ("Plaintiffs"), on behalf of themselves and all others similarly situated (collectively, the "Customers" or "Class," as hereinafter defined), upon personal knowledge as to the facts pertaining to them and upon information and belief as to all other matters, based on the investigation of their counsel, including information learned from confidential witnesses, bring this class action against Sony Corporation of America, Inc. ("SCA"), a New York corporation; Sony Computer Entertainment America, LLC ("SCEA"), a Delaware limited liability company; Sony Pictures Entertainment, Inc. ("SPE"), a Delaware corporation; and Sony Network Entertainment International, LLC ("SNEI") (collectively "Defendants" or "Sony"), and allege as follows:

INTRODUCTION

1. This is a nationwide class action for damages and injunctive relief arising from one of the largest data breaches in United States history. On or about April 16, 2011, Sony sustained a massive breach to its inadequately secured PlayStation Network, which placed personal information belonging to *77* ***million*** user accounts in the hands of cyber-criminals. Dr. Paul Judge, chief research officer and vice president of Barracuda Networks, has stated that the intrusion is "arguably the second largest data breach ever," and that "the most troubling thing about this breach is the breadth of data that was leaked."

2. The shear breadth of data that was stolen is, in fact, astounding, and includes sensitive, personal identification and financial information, such as the following confidential data: customer names, mailing addresses, email addresses, birth dates, credit card numbers and expiration dates, online network passwords, login credentials and other personal information (collectively, "Personal Information").

3. Even more incredible, according to information provided by industry experts and confidential informants (described below), Sony knew that its inadequate security systems placed it at an increased risk for the attack, which directly and proximately caused the theft of its Customers' Personal Information and a month-long interruption of the PlayStation and SPE Networks (defined below).

4. According to numerous confidential witnesses cooperating in the investigation of this action and based upon their firsthand knowledge:

(a) Sony took numerous precautions and spent lavishly to secure its proprietary development server containing its own sensitive information, including the installation of appropriate firewalls, IP address limitations and updated software, but recklessly declined to provide adequate protections for its Customers' Personal Information;

(b) Sony implemented enhanced measures for its own proprietary systems at the expense of safeguarding its Customers' Personal Information and that these disparities existed because Sony wanted to "protect [itself] and not the people that use [its] servers;"

(c) In fact, protecting its own development server was Sony's "number one concern;"

(d) Sony chose to never install a firewall on the PlayStation and SPE Networks, and only implemented firewalls on an *ad-hoc* basis when it determined that a particular user was attempting to gain unauthorized access;

(e) Sony sought to cut its costs at the expense of its Customers by terminating a significant number of employees immediately prior to the security breach, including personnel responsible for maintaining the security of the Network;

(f) Sony knew that security on its Network was weak because it had experienced hackings of sensitive data on a smaller scale prior to the massive security breach;

(g) Sony's gaming consoles have the same access number, rendering them more prone to data breaches since access to a single unit provides access to all; and

(h) Sony took unnecessary risks with its Customers' Personal Information by storing credit card information in an insecure manner.

5. Critically, according to Confidential Witness 1, a former Sony employee who was with SCEA from 2006 to 2008 and Sony Online Entertainment April 2010 to August 2010, Sony invested significant resources, including firewalls, a debug unit and IP address limitations, to protect its own confidential proprietary information housed on Sony's "development server," known internally as "the PS DevNetwork." According to this witness, these measures made it "extremely

difficult" to breach the PS DevNetwork. While Sony knew that these basic security measures were necessary to protect its proprietary systems, it chose to cut corners when it came to its Customers' Personal Information and failed to implement similar safeguards on the PlayStation and SPE Networks. Indeed, the Playstation and SPE Networks lacked basic security measures such as updated software, adequate encryption and fire walls. As a direct result of Sony's knowing failure to adequately protect its Customers' data, hackers were able to steal Customers' Personal Information on an epic scale.

6. Additional confidential information indicates that Sony knew that its systems were already insecure. According to an email sent to Sony *two months* prior to the breach, there was widespread hacking of the Network. Sony was specifically warned by Network user, Eugene Alvarado, that there was "a security vulnerability, especially with console information."

7. Sony facilitated the massive data breach by, among other things, making its systems susceptible to multiple security breaches by deceptively and unlawfully designing, manufacturing, distributing, marketing, selling and warranting defective electronic systems and equipment, such as the Sony PlayStation (collectively the "Equipment"), and defective on-line services, including the SPE Network ("SPE Network") (www.sonypictures.com) and the Sony PlayStation Network's Qriocity. Qriocity is a trade name for Sony's streaming music, games, e-book, and video-on-demand services, and is available exclusively through the PlayStation Network. The PlayStation Network and Qriocity are collectively referred to as the "PlayStation Network" or the "Network."

8. Although Sony was fully aware of the massive breach by April 20, 2011, it did not disclose the breach to its Customers until April 26, 2011, stating on its official PlayStation weblog that "an illegal and unauthorized person" obtained its Customers' Personal Information." This prolonged ten-day delay (from the time the Network was breached until the time Sony disclosed it) effectively prevented Sony Customers from taking prompt and reasonable steps to attempt to secure their Personal Information from identity theft and other financial crimes.

9. Sony took the PlayStation Network offline and kept it offline for 30 days while it investigated the breach. Online games and services are an essential component of the PlayStation

Network and, thus, the breach and Sony's subsequent conduct substantially impacted the playing experience of the online gaming community.

10. On April 26, 2011, Sony finally disclosed on its official PlayStation weblog that an "illegal and unauthorized person" obtained its Customers' Personal Information.

11. On May 3, 2011, USA Today reported a second data breach incident involving another Sony division. This incident occurred on April 16 and 17, 2011, and involved approximately 23,400 financial records from an outdated 2007 database encompassing Sony account holders outside the United States.

12. On June 3, 2011, Sony's SPE Network was also breached and the Personal Information of at least tens of thousands of Customers was similarly stolen. LulzSec, the group claiming responsibility for the attack, stated that it obtained the data using unsophisticated tools and posted Customers' Personal Information, including the email address and password of Plaintiff Jacques Daoud Jr., on its website as proof that it had in fact obtained this information.

13. Plaintiffs Felix Cortorreal, Jacques Daoud Jr. and Jimmy Cortorreal bring this lawsuit on behalf of themselves and all others in the United States who were active subscribers to the PlayStation Network and/or Qriocity services on April 16 and 17, 2011 or the SPE Network on June 3, 2011, and allege that Sony violated California's Consumer Legal Remedies Act, Cal. Civ. Code §§1750 *et seq.*, California's Unfair Competition Law, Cal. Bus. & Prof. Code §§17200 *et seq.*, the Federal Electronic Communications Privacy Act, 18 U.S.C. §§2702 *et seq.*, and common law claims for negligence, breach of contract, and breach of fiduciary duty. Plaintiffs seek monetary damages, restitution and injunctive relief.

PARTIES

14. Plaintiff Felix Cortorreal is a resident of Nassau County, New York, who purchased Equipment from Sony and was a member of the PlayStation Network on April 16 and 17, 2011.

15. Plaintiff Jacques Daoud Jr. is a resident of Kings County, New York, who purchased Equipment from Sony and was a member of the SPE Network on June 3, 2011.

16. Plaintiff Jimmy Cortorreal is a resident of Queens County, New York, who purchased Equipment from Sony and was a member of the PlayStation Network on April 16 and 17, 2011.

17. As subscribers of the PlayStation Network or SPE Network, Plaintiffs provided certain Personal Information to Sony, including credit card numbers and passwords, which Sony kept on file to pay for initial sign-up fees and to facilitate purchases of "add-ons." This information was provided by Plaintiffs, as requested by Sony, and as required by Sony, to avail themselves of its services. Plaintiffs' usage data, relating to their purchases and online activity at the Network, were stored and maintained by Defendants. Due to Defendants' wrongdoing and violations of their privacy rights, Plaintiffs' and Class members' Personal Information has been severely compromised, leaving them exposed to increased risk of fraud, identity theft and other financial crimes. Moreover, Plaintiffs lost access to the PlayStation Network for a month, significantly decreasing the value of the Equipment they purchased for the purpose of online gaming.

18. Defendant SCA is a New York corporation with its headquarters at 550 Madison Avenue, 27th Floor, New York, New York 10022.

19. Defendant SCEA is a Delaware limited liability company and is a wholly-owned subsidiary of SCA. Its executive offices and corporate headquarters are located at 919 East Hillside Boulevard, Foster City, California 94404. It also maintains offices at 1630 Stewart Street, Studio A, Santa Monica, California 90404. SCEA serves as headquarters for all North American operations and is responsible for PlayStation product sales in the United States, Canada and Latin America.

20. Defendant SPE is a Delaware corporation and a wholly-owned subsidiary of SCA. Its executive offices and corporate headquarters are located at 10202 West Washington Boulevard, Culver City, California 90232.

21. Defendant SNEI is a Delaware limited liability company with its executive offices and corporate headquarters at 6080 Center Drive, Los Angeles, California 90045.

JURISDICTION AND VENUE

22. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act of 2005, 28 U.S.C. §§1332(d), 1453, and 1711–1715, as (a) the Class has more than 100 members; (b) at least one of the members of the Class is a citizen of a state other than California; and (c) the claims of the individual Class members in the aggregate exceed the sum value of $5,000,000, exclusive of interests and costs.

23. This Court has personal jurisdiction over the Defendants pursuant to *International Shoe Co. v. Washington*, 326 U.S. 310, 316 (1945), and its progeny, because (a) a substantial portion of the wrongdoing alleged in this Complaint took place in this District; (b) Defendants are authorized to do business in this District; (c) Defendants have sufficient minimum contacts with this District; and (d) Defendants intentionally avail themselves of the consumer markets in this District through the promotion, marketing, and sales of its Equipment and Network in this District.

24. Venue is proper in this District under 28 U.S.C. §1391 because one or more Defendants are located in this District and because a substantial part of the events or omissions giving rise to the claim occurred in this District.

FACTUAL ALLEGATIONS

A. Background

25. The PlayStation brand, which was created and developed by SCA and SCEA, consists of video game consoles, a media center, an online service, a line of controllers, a handheld device and multiple magazines. It is one of the most popular gaming systems purchased worldwide.

26. The PlayStation Network is an online service that allows users to play games with other players both in person and online. The PlayStation Network includes an online virtual market known as the "PlayStation Store," which allows the purchase and downloading of games and various forms of multimedia, a subscription-based online service known as "PlayStation Plus," and a social gaming networking service called "PlayStation Home." Sony has also partnered with third-party vendors such as Netflix and Hulu to provide streaming media content, including movies and television shows, directly to a user's console for a monthly access fee. To take advantage of any of the services the Network offers, Customers are required to provide a valid credit card number and other Personal Information.

27. Sony Customers use a majority of Defendants' multimedia Equipment (including PlayStation 3, PlayStation Portable System, Bravia Entertainment Television Systems, Sony Personal Computers, and Sony Blu-Ray Disk Players) to access the PlayStation Network through an internet connection.

28. Access to the basic Network is provided for free to Sony Customers who purchase the Equipment. However, Sony's Equipment is priced significantly higher than its principal competitor, Microsoft's Xbox.

29. Even though access to the Network is free, combined revenue from the PlayStation Store, PlayStation Plus, PlayStation Home, and third-party vendors makes the Network one of SCEA's largest sources of revenue, earning an estimated $850 million annually. According to Nielson data, as of October 2010, almost half of all PlayStation games are played online via the Network. The use and availability of the Network is central to most users of PlayStation Equipment, including Plaintiffs and the Class. For example, a number of PlayStation 3 games, including the popular *Call of Duty* and *Madden NFL*, are specifically designed to be played online with, in some cases, up to 20 other users. Without the Network, the PlayStation Equipment and a number of PlayStation games are worth significantly less to Sony Customers.

30. As part of the registration process to join the Network, individuals are required to provide their Personal Information to Defendants by creating a "Master" account. Through his or her "Master" account, an individual is required to store credit or debit card information in an online "Wallet" for purposes of initial sign-up and to facilitate future online purchases. Sony maintains this Personal Information, including the information contained in a Sony Customer's Wallet, in a database on its internal network servers. Sony also tracks its Customers' usage of the Network ("Usage Data"), and that Usage Data is stored on internal network servers.

B. Sony Falsely Touted Its Network as Secure While Simultaneously Failing to Implement Basic Security Measures

31. Sony made repeated assertions to its Customers that it would take reasonable and appropriate measures to protect their Personal Information.

32. On the SCA website page entitled "Terms of Use/Security," SCA states in relevant part:

> Security
>
> While SCA cannot guarantee that unauthorized access will never occur, rest assured that SCA takes great care in maintaining the security of your personal information and in preventing unauthorized access to it through the use of appropriate technology and internal procedures.

33. Sony's current PlayStation Privacy Policy states:

> Accuracy & Security
>
> We take reasonable measures to protect the confidentiality, security, and integrity of the personal information collected from our website visitors. Personal information is stored in secure operating environments that are not available to the public and that are only accessible to authorized employees. We also have security measures in place to protect the loss, misuse, and alteration of the information under our control.

34. As discussed herein, Sony never implemented appropriate security measures and left its Customers vulnerable to one of the largest cyber attacks and data thefts in United States history.

C. Despite Sony's Assertions to the Contrary, Its Network Was Inadequately Protected and Left Vulnerable to a Security Breach

35. Despite Sony's representations that it took reasonable steps to secure its Network, it in fact failed to take reasonable and adequate measures to protect Customers' Personal Information stored on its Network. Sony specifically failed to, among other things, install appropriate firewalls on the Network, update its software, or properly encrypt certain Personal Information.

36. As a leader in the computer technology industry, Sony had the ability and know-how to implement and maintain sufficient online security. While Sony implemented security to protect its own proprietary systems, it failed to capitalize on its expertise as a technology leader and implement similar security measures to protect its Customers' Personal Information.

37. According to Confidential Witness 1, Sony invested significant resources, including firewalls, debug programs, and IP address limitations, to protect its own confidential proprietary information housed on Sony's "development server," without incorporating the same safeguards on the Network (such as a basic firewall). Access to the former could cause the ***company*** financial ruin, while access to the latter could cause the financial ruin of ***millions*** of unsuspecting Customers.

38. According to Confidential Witness 1, "Sony was more concerned about their development server being hacked rather than some consumer's data being stolen. They want to protect themselves and not the people that use their servers."

39. Gene Spafford, a computer science professor at Purdue University, testified to the inadequacy of Sony's security measures at a Congressional hearing on May 4, 2011 entitled "The Threat of Data Theft to American Customers," which was convened to "examine risks related to data

breaches, the state of ongoing investigations, current industry data security practices, and available technology." Professor Spafford concluded that, based upon reports in the press and discussions at professional meetings, Sony used "outmoded, flawed software" and "fail[ed] to follow some basic good practices of security and privacy."

40. Professor Spafford further testified that it was his understanding, based upon widespread media reports and industry websites, that Sony had failed to install a firewall on its Network.

41. Sony's failure to install a firewall was confirmed by Confidential Witness 2, a Platform Support Engineer for Sony Online Entertainment from 2006 until March 2011. According to this witness, Sony's technicians only installed firewalls on an *ad-hoc* basis after they determined that a particular user was attempting to gain unauthorized access to the Network.

42. Sony's decision not to install a firewall on its Network diverged from widespread industry practice and standards, including the Payment Card Industry Data Security Standard ("PCI-DSS"), which requires anyone collecting payment card information to install and maintain a firewall.

43. Subsequent to his testimony before Congress, Professor Spafford explained that Sony's backend servers, which are used for registering and storing Personal Information, were running outmoded software, and it is these servers which provided an entry point for the persons who hacked into the Network in April 2011.

44. The adequacy of Sony's purported encryption of certain Personal Information has also been called into question. Sony has never disclosed what methods it uses to encrypt credit card information. This lack of transparency has led some information technology specialists to conclude that any encryption is either weak or easily broken.

45. Sony entirely failed to encrypt other sensitive, and arguably more critical, Personal Information, including Customers' passwords and email addresses. This information was "transformed using a cryptographic hash function," a type of digital fingerprint that is particularly vulnerable to security breaches.

46. Sony's failure to encrypt certain Personal Information, such as Customers' passwords, has fueled intense criticism from industry experts. Technology security experts at

Attrition.org have stated that Sony's lack of encryption when storing Customers' personal details and passwords was both "reckless and ridiculous." These experts went on to explain that "even security books from the '80s were adamant about encrypting passwords at the very least."

47. Sony also needlessly stored its Customers' credit card information. According to Confidential Witness 3, a former SCEA Quality Assurance Tester from February 2008 to May 2010, Sony took an unnecessary risk by storing Customers' credit card information, which departs from the practice of its principal competitor and exposes the Personal Information of its Customers to additional data security risks.

48. According to Confidential Witness 4, a former Quality Assurance Analyst with Sony Online Entertainment from January 2010 to March 2011, SCEA, the division responsible for the PlayStation 3 console and Network, was not nearly as secure as Sony Online Entertainment.

49. The PlayStation 3 console itself may also unnecessarily compromise data security. Confidential Witness 4 explained that PlayStation 3 consoles are supposed to be secured by a "random number generator," but are not. Indeed, each console has the same access number – rendering the Equipment particularly susceptible to security breaches since access to one provides access to all.

50. On June 8, 2011, Sony deputy president, Kazuo Hirai, essentially admitted that Sony's Network did not meet minimum security standards. When asked whether Sony had revised its security systems as a result of the massive breach that occurred in April 2011, Mr. Hirai stated that Sony has "done everything to bring our practices at least in line with industry standards or better."

D. Beginning in April 2011, Sony Failed to Prevent and Delayed Disclosing a Massive Security Breach of Its Network

51. On or about April 16, 2011, Sony Customers noticed intermittent interruptions to the Network. Unbeknownst to them, the outages were caused by a massive security breach of the Network, allegedly undertaken by a group of hackers collectively known as "Anonymous." This breach would not have occurred had Sony maintained adequate or sufficient security measures to prevent unauthorized access to its Customers' sensitive Personal Information.

52. It took Sony at least two days to even detect the massive security breach that led to the data theft of almost a hundred million Customers' Personal Information.

53. On or about April 19, 2011, Sony learned that its Network had been compromised, but did not disclose this to its Customers.

54. On April 20, 2011, Sony took the unprecedented step of taking the Network offline. At the same time, it issued the following statement: "We're aware certain functions of PlayStation Network are down. We will report back here as soon as we can with more information." The statement did not mention the security data breach that had occurred, nor were Customers informed that their Personal Information had been compromised or stolen.

55. Even though Sony was aware of the massive security breach no later than April 20th, it was not until an entire week later, on April 26, 2011, that Sony disclosed the breach for the first time, stating:

> Although we are still investigating the details of this incident, we believe that an unauthorized person has obtained the following information that you provided: name, address (city, state, zip), country, email address, birthdate, PlayStation Network/Qriocity password and login, and handle/PSN online ID. It is also possible that your profile data, including purchase history and billing address (city, state, zip), and your PlayStation Network/Qriocity password security answers may have been obtained. If you have authorized a sub-account for your dependent, the same data with respect to your dependent may have been obtained. While there is no evidence at this time that credit card data was taken, we cannot rule out the possibility. If you have provided your credit card data through PlayStation Network or Qriocity, out of an abundance of caution we are advising you that your credit card number (excluding security code) and expiration date may have been obtained.

Sony cautioned its Customers to watch out for unauthorized use of credit card data as well as identity-theft scams as a result of the theft, and encouraged its Customers to "remain vigilant to review your account statements and to monitor your credit or similar types of reports."

56. On June 3, 2011, despite the massive breaches that had already occurred, Sony again failed to protect its Customers' Personal Information from being stolen by persons using an elementary hacking device known as an "SQL Injection." According to LulzSec, the hacking collective claiming responsibility for the incident, this method is "one of the most primitive and common vulnerabilities." The group further claimed that from a "single injection" it "accessed

EVERYTHING" and that it was able to do so "easily" and "without the need for outside support or money." (emphasis in original).

57. Even more damning, the LulzSec group claimed that the data it stole was not encrypted, not hidden behind a cryptographic hash tag, and flagrantly stored in plaintext. The group also posted on its website certain hijacked Personal Information, including email addresses and passwords, of thousands of Sony Customers, specifically including that of Plaintiff Jacques Daoud Jr.

58. The information obtained from this data breach has already led to widespread hacking of Personal Information belonging to Plaintiffs and the Class on a multitude of other websites.

59. For example, Plaintiff Jacques Daoud Jr. has been notified by both Twitter and Facebook that his account may have been compromised.

E. Sony Had Been Repeatedly Warned that Its Network Was Vulnerable to Attack

60. Sony knew or should have known that its out-of-date and inadequate technology would leave its Network databases vulnerable to such attacks. However, Sony failed to take corrective measures to update the technology, even after prior security breaches and in the face of a direct threat by a hacking collective to infiltrate the Network.

61. Sony's PlayStation Network had been compromised by unauthorized users a number of times before the massive security breach at issue here. For example, in May 2009, reports surfaced that unauthorized copies of Customers' credit cards were emailed to an outside account. And in January 2011, hackers made PlayStation game *Modern Warfare 2* unplayable online.

62. Confidential Witness 5, a former Senior Project Coordinator for SCEA from June 2000 until March 2011, expressed his utter lack of surprise that the Network was breached in April 2011, since he and others at Sony knew it had been breached on prior occasions as well.

63. On one such instance in February 2011, Eugene Alvarado, an account holder and frequent online gamer, reported to Sony that there was widespread hacking of the Network which was interfering with his and other Customers' use thereof. Alvarado used the online complaint form located on Sony's website to inform Sony that his console had been breached, affecting his ability to

play certain PlayStation games and degrading his customer experience. Mr. Alvarado wrote: "As a network Admin, it posses [sic] a security vulnerability, especially with console information."

64. In late 2010 and early 2011, a 19-year old man named George Hotz also successfully "jailbroke" the PlayStation 3 console and created an "exploit" – software or data that takes advantage of a vulnerability in a network to compromise the network and gain control of the system. Hotz's exploit allowed him to modify the PlayStation 3 console and use it with other operating systems, like Linux, to play "homebrewed" games. Such modification is relatively common among high-tech gamers, and other console manufacturers, such as Microsoft, have silently acquiesced to the practice. Indeed, earlier versions of the PlayStation console allowed users to modify the Equipment without resorting to such jailbreaks.

65. Hotz publicly disclosed his exploit and Sony subsequently sued him for copyright infringement. In response to Sony's lawsuit against Hotz, the hacker collective known as "Anonymous" announced its outrage with the company and publicly stated that it planned to attack the PlayStation Network.

66. Just two weeks prior to the breach, Anonymous sent the following message to Sony:

> You have abused the judicial system in an attempt to censor information on how your products work . . . Now you will experience the wrath of Anonymous. You saw a hornet's nest and stuck your [expletive] in it. You must face the consequences of your actions. Anonymous style . . . ***Expect us*** (emphasis added).[1]

67. Despite Anonymous' direct threat to imminently breach the Network, Sony failed to implement basic safeguards to protect the Personal Information of its Customers.

68. Moreover, just two weeks before the April breach, Sony laid off a substantial percentage of its Sony Online Entertainment workforce, including a number of employees in the Network Operations Center, which, according to Confidential Witness 2, is the group that is responsible for preparing for and responding to security breaches, and who ostensibly has the skills to bring the Network's security technology up-to-date.

---

[1] The term "expect us" is Anonymous's signature catch phrase and is frequently used by the group to signal an impending attack.

E. Industry Experts, Academics and United States Senators Have Openly Criticized Sony for Failing to Adequately Protect the Personal Information of Its Customers

69. Since the security breach, Sony has represented that it finally implemented basic measures to defend against new attacks, including the following systems that should have already been in place: automated software monitoring, enhanced data encryption, enhanced ability to detect intrusions to the Network, such as an early-warning system to detect unusual activity patterns, and additional firewalls. In addition, Sony hired a Chief Information Security Officer, a position that is very common in Fortune 500 companies.

70. All of these new measures should have been in place before the massive security breach. Confidential Witness 6, a Product Service Manager at SCEA from January 2005 until March 2011, likened these measures to "getting an alarm system installed after you have been burglarized."

71. According to Professor Spafford, Sony should have had the appropriate tools in place that would have enabled it to identify a breach almost immediately, especially since Sony had a history of break-ins to its sites worldwide. In Professor Spafford's professional judgment, "Sony should have been more aware of this then they seem to have been."

72. John Bumgarner, Chief Technology Officer of the independent, non-profit research institute United States Cyber-Consequences Unit, found that as of May 10, 2011, the PlayStation Network was still vulnerable to attacks. Specifically, unauthorized users could still access internal Sony resources, including security-management tools.

73. Mr. Bumgarner was correct, and the SPE Network was breached on June 3, 2011. LulzSec, the hacking collective that claimed responsibility for the incident, stated that its motivation was to show that Sony lied when it told Customers that it had revamped security to protect against the same type of attack that occurred in April 2011. Indeed, numerous experts in the field attribute this data breach to an unsophisticated method of hacking which would not have been successful if even the most basic security measures were in place.

74. According to Tony Bradley, a PCWorld journalist who covers technology issues, in an article entitled, "Sony Hacked Again: How Not To Do Network Security," Sony "seems to ignore compliance requirements and basic security best practices, so it is basically begging to be attacked."

Bradley advised that companies should follow security "best practices and data security compliance requirements" – and in short – "[d]on't be Sony."

75. According to Randy Abrams, director of technical education for ESET, a software company specializing in data security, if Sony did in fact store passwords in plain text it would be nothing short of "blatant negligence."

76. Similarly, according to Fred Touchette of AppRiver, an email and web security software provider:

> There is no doubt that Sony needs to spend some major effort in tightening up its network security. This latest hack against them was a series of simple SQL injection attacks against its web servers. This simply should not have happened.

77. Sony's delay in reporting the breach to the public also sparked intense outrage, causing U.S. Senator Richard Blumenthal (D-CT) to condemn Sony's lack of reasonable security measures. "Sony persists in unconscionably refusing to alert its millions of users on the PlayStation Network proactively, while they remain at serious risk of identity theft and other financial attacks stemming from their personal and financial data having been compromised."

78. Gamers have similarly expressed their unhappiness and dissatisfaction with Sony's conduct, none more so than the editors of the gamer website IGN.com:

(a) Hilary: "[I]t's disheartening to see a company respond so poorly to the biggest crisis it's faced this console generation . . . Faced with a crisis that affected its customers, people at Sony ignored compassion, eschewed openness and instead hid in silence . . .While your credit card info may have been exposed to criminals that brought down Sony's service, leaving those loyal to PlayStation in potential financial peril, executives chose to keep their mouths shut . . . Their true selves were revealed – as selfish, greedy, self-centered individuals more concerned with the bottom line than the value of their customer base."

(b) Charles: "It shouldn't have taken this long for Sony to issue a statement about this kind of thing. Customer security should be the number one priority if Sony wants its consumer base to maintain faith in its service."

(c) Tom: "[F]or Sony to wait 6 whole days before holding their hands up to admit 75 million people's PSN details - including credit card details - could have been compromised, is galling to say the least. This is a scandal of epic proportions."

F. Sony's Failure to Implement Adequate Security Measures Has Victimized Almost a Hundred Million Customers Who Entrusted Sony with Their Personal Information

79. As a result of these breaches to both the PlayStation and SPE Networks, cyber-criminals now possess the Personal Information of many millions of Sony Customers. While credit card companies offer protection against unauthorized charges, the process is long, costly and frustrating. Physical cards must be replaced, credit card information must be updated on all automatic payment accounts, and victims must add themselves to credit fraud watch lists, which substantially impairs their ability to obtain additional credit. Immediate notice of the breach is essential to obtain the best protection afforded by these services.

80. In addition to identity theft, unauthorized persons can use the Personal Information in a variety of ways. According to various studies, anywhere between 60 and 75% of individuals use the same password on multiple websites, including financial institution websites. According to Troy Hunt, a software architect, 92% of users actually victimized by the SPE Network attack used the same passwords for other accounts registered under the same email addresses. As such, Customers' Personal Information used for these other services has been seriously compromised.

81. As alleged above, Plaintiff Jacques Daoud Jr.'s (and that of numerous members of the Class) Personal Information has already been compromised; he has suffered security beaches on multiple online accounts and his email address and password has been made public on several websites.

82. Information about Customers may also be used to harass or stalk them. And the threat of "spear phishing" – where details of a Customer's Usage Data can be used to tailor a "phishing" message that looks authentic, but is actually a ruse to get the Customer to divulge account information – is very real. In sum, the ability of cyber criminals to access Sony Customers' Personal Information has seriously impacted the safety and security of Customers' Personal Information, causing potential financial loss, harassment or worse.

83. Customers' email addresses have been sold to spammers and the resulting spam now clogs Customers' inboxes.

84. The PlayStation Network remained offline for 30 days while Sony conducted an audit of its systems to determine exactly how the breach occurred. During this prolonged period when Sony took the Network offline, Customers were unable to access their online accounts, use third-party provider services such as Netflix, purchase "add-ons" with their virtual Wallets and, most importantly, play multi-player online games. For Plaintiffs and the members of the Class, this significantly lessened the value of their Equipment which they purchased with the expectation that the Network would be accessible 24 hours a day, 7 days a week, for services like online gaming, store purchases, game downloads, and third-party provider services.

CLASS ACTION ALLEGATIONS

85. Plaintiffs bring this action on behalf of themselves and a nationwide class of persons ("Class"), defined as follows:

> All persons in the United States who were active subscribers to the PlayStation Network or Qriocity service on or about April 16 and 17, 2011 or SPE's Network on or about June 3, 2011, excluding: Defendants; any affiliate, parent or subsidiary of Defendants; any entity in which Defendants have a controlling interest; any officer, director or employee of Defendants; any successor or assign of Defendants.

86. This action has been brought by and may properly be maintained on behalf of the Class defined above under the criteria of Rule 23 of the Federal Rules of Civil Procedure.

87. Members of the Class are so numerous that their individual joinder herein is impracticable. Plaintiffs believe that the Class members number in the tens of millions, based on reports of the number of Network accounts in existence at the time of the breach.

88. Common questions of law and fact exist as to all members of the Class and predominate over questions affecting only individual Class members. These common questions include the following:

(a) Whether Sony's Equipment and Network were defectively designed, marketed, distributed, and sold;

(b) Whether Sony knew or should have known that its Equipment and Network were defectively designed, marketed, distributed, and sold;

(c) Whether Sony knowingly concealed the defective nature of its Equipment and Network;

(d) Whether Sony's marketing was designed to lead Customers to believe that use of the Network was secure;

(e) Whether Sony's marketing of the Network was reasonably likely to mislead or deceive Customers;

(f) Whether Sony misrepresented the safety, security and usefulness of the Equipment and Network;

(g) Whether Sony knowingly concealed from the public information regarding the security breaches that occurred on its PlayStation Network;

(h) Whether Sony's conduct is unfair and/or deceptive and therefore violates California's Consumer Legal Remedies Act, Cal. Civ. Code §§1750 *et seq.*;

(i) Whether Sony's conduct is unlawful, unfair or fraudulent and therefore violates California's Unfair Competition Law, Cal. Bus. & Prof. Code §§17200 *et seq.*;

(j) Whether Sony's conduct violated the Federal Electronic Communications Privacy Act, 18 U.S.C. §§2702 *et seq.*;

(k) Whether Sony was negligent and breached its duty to protect Customers' Personal Information;

(l) Whether Sony breached its agreements with Customers; and

(m) Whether Sony breached its fiduciary duty to Customers.

89. Plaintiffs' claims are typical of the claims of the Class as the claims of Plaintiffs and all Class members arise from the same set of facts regarding Defendants' failure to protect Class members' Personal Information.

90. Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the members of the Class they seeks to represent. Plaintiffs have retained counsel competent and experienced in complex Class action litigation, and Plaintiffs intend to prosecute this action vigorously. The interests of members of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

91. The class action is superior to other available means for the fair and efficient adjudication of this dispute. The injury suffered by each individual Class member is not large enough to make the prosecution of individual actions against Sony economically feasible, and the filing of millions of individual actions would be inefficient, wasteful of resources, and create huge delays in adjudicating these issues, for the courts, as well as for Customers. Individual litigation also creates a potential for inconsistent or contradictory judgments. The Class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

92. In the alternative, the Class may be certified because:

(a) Sony has acted on grounds generally applicable to the Class, thereby making appropriate injunctive relief with respect to the members of the Class as a whole;

(b) The prosecution of separate actions by the individual member of the Class would create a risk of inconsistent or varying adjudications with respect to individual Class members which would establish incompatible standards of conduct for Sony; and

(c) The prosecution of separate actions by individual Class members would create a risk of adjudications with respect to them which would, as a practical matter, be dispositive of the interests of other Class members not parties to the adjudications, or substantially impair or impede their ability to protect their interests.

COUNT I

Violation of California's ConsumerS Legal Remedies Act ("CLRA") (California Civil Code §§1750, *et seq.*)

93. Plaintiffs hereby incorporate by reference each and every allegation set forth herein.

94. The CLRA was enacted to protect consumers against unfair and deceptive business practices. It extends to transactions that are intended to result, or which have resulted, in the sale or lease of goods or services to consumers. Sony's conduct falls within the CLRA because the design, development, and marketing of Sony's Equipment and Network services are intended to and did result in sales of the Equipment and Network services.

95. The acts, omissions, misrepresentations, and practices of Sony were and are likely to deceive Customers. By misrepresenting the safety and security of their Equipment and Network, Sony violated the CLRA. Sony had exclusive knowledge of undisclosed material facts, namely, that its Network was defective, and withheld that knowledge from Customers.

96. Sony maintained a database of Customers' Personal Information and represented to its Customers that such database was secure and would remain private. Sony engaged in deceptive acts and business practices with respect to Customers by providing in its Privacy Policy that it uses "reasonable measures to protect the confidentiality, security, and integrity of the personal information collected from our website visitors" and that it maintains security measures "to protect the loss, misuse, and alteration of the information under our control."

97. However, Sony knew or should have known that it did not employ reasonable measures that would have kept Customers' Personal Information secure and prevented the loss or misuse of Customers' sensitive data. For example, Sony failed to use a sufficient encryption code to protect Customers' financial information and failed to employ any encryption whatsoever to protect other Personal Information, such as email addresses and passwords.

98. Sony's deceptive acts and business practices induced Plaintiffs and the Class to register for the Network and provide sensitive Personal Information, including credit card information, for the purchase of content from the PlayStation Store. But for these deceptive acts and business practices, Plaintiffs and the Class would not have purchased the Equipment or services from the Network, or in the alternative, would not have provided Sony with the sensitive Personal Information.

99. Sony also engaged in deceptive acts and business practices with regard to Plaintiffs and Class members by failing to timely notify them that their Personal Information had been stolen.

100. As a direct and proximate result of Sony's deceptive acts and business practices as alleged herein, Plaintiffs and members of the Class have suffered injury-in-fact and lost money or property, including the theft of their valuable Personal Information.

101. Plaintiffs seek an order enjoining Defendants from the unlawful practices described herein, a declaration that Sony's conduct violates the CLRA, restitution as appropriate, and attorneys' fees and costs of litigation.

102. Pursuant to §1782 of the CLRA, Plaintiffs notified Defendants in writing of the particular violations of §1770 of the CLRA and demanded that Defendants rectify the actions described above by providing complete monetary relief, agreeing to be bound by their legal obligations and to give notice to all affected customers of their intent to do so. Plaintiffs sent this notice by certified mail, return receipt requested, to Defendants' principal places of business.

103. If Defendants fail to adequately respond to Plaintiffs' demand within 30 days of the letter pursuant to §1782 of the Act, Plaintiffs will amend this claim to add additional claims for relief, including claims for compensatory and exemplary damages. Plaintiffs are already entitled to the relief set forth above, along with costs, attorneys' fees and any other relief which the Court deems proper.

COUNT II

Violation of California's Unfair Competition Law ("UCL") (California Business and Professions Code §§17200 *et seq.*)

104. Plaintiffs hereby incorporate by reference each and every allegation set forth herein.

105. Pursuant to the UCL, "unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising."

106. Sony directly violated the UCL by misrepresenting the quality of its Network, specifically the security thereof, and its ability to safely store Customers' Personal Information. Sony stated in its Privacy Policy that it would take "reasonable measures" to protect Customers' Personal Information against breaches in security, but clearly failed to do so. It used weak or no encryption and failed to install and maintain firewalls, in violation of the PCI-DSS. Sony was aware of previous attempts to break into its systems but failed to rectify the glitches that allowed for those breaches to be successful.

107. Sony also violated the UCL by intentionally and knowingly causing injury to its Customers by failing to immediately notify Customers of the security breach. If the Customers had

been notified in a timely fashion, they could have taken appropriate precautions to safeguard their Personal Information.

108. These fraudulent and deceptive practices, including their misrepresentations regarding network security, have deceived members of the public.

109. As a direct and proximate result of Sony's conduct as alleged herein, Plaintiffs and members of the Class have suffered injury-in-fact and lost money or property, including the theft of their valuable Personal Information.

COUNT III

Violation of the Electronic Communications Privacy Act (18 U.S.C. §2702 *et seq.*)

110. Plaintiffs hereby incorporate by reference each and every allegation set forth herein.

111. The Electronic Communications Privacy Act ("ECPA") is a federal statute that provides a private civil right of action to customers when a company mishandles their electronically stored information.

112. The ECPA prohibits "a person or entity providing an electronic communication service to the public [from] knowingly divulg[ing] to any person or entity the contents of a communication while in electronic storage by that service," and similarly prohibits "a person or entity providing remote computing service to the public [from] knowingly divulg[ing] to any person or entity the contents of any communication which is carried or maintained on that service."

113. As a provider of the PlayStation Network, Sony is clearly "a provider of remote computing services." The Network "[provides] to the public [ ] computer storage or processing services by means of an electronic communications system." An "electronic communications system" is "any service which provides to users thereof the ability to send or receive wire or electronic communications." And "electronic communications" are defined as "any transfer of … data… transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." Sony's Network provides Customers the ability to send electronic communications and stores data that Customers transfer to

it, including Plaintiffs' and Class members' sensitive Personal Information. It is therefore a violation of the ECPA to cause the dissemination of such data.

114. By failing to enact commercially reasonable or adequate measures to protect the dissemination of Plaintiffs' and Class members' Personal Information and knowing that such failure could result in a breach of its security, Sony caused and otherwise facilitated unauthorized users' breach of security, thus knowingly divulging information in violation of the ECPA.

115. As a direct and proximate result of Sony's violation, Plaintiffs and members of the Class have suffered injury-in-fact and lost money or property, including the loss of their ability to access the Network and the theft of their valuable Personal Information.

COUNT IV

Negligence

116. Plaintiffs hereby incorporate by reference each and every allegation set forth herein.

117. By receiving Plaintiffs' and Class members' Personal Information in exchange for Equipment and Network services, Sony assumed a duty to safeguard that data by enacting commercially reasonable security measures to prevent unauthorized access to the database of Personal Information. That duty included, but was not limited to, hiring and retaining trustworthy and capable employees and properly designing, maintaining, and testing their security systems. Sony had a further duty to implement processes that would detect a breach in its security system in a timely manner and to inform the public in a timely manner when such a breach was in fact detected.

118. Sony was negligent in its duty to safeguard the Personal Information:

(a) Sony improperly stored Personal Information on its Network. Sony failed to use reasonable or sufficient encryption and/or other common forms of data protection to safeguard against unauthorized access.

(b) Sony failed to reasonably monitor the Network and allowed for unauthorized access of Plaintiffs' and Class members' Personal Information.

(c) Sony failed to recognize in a timely manner that its systems had been breached.

(d) Sony did not disclose the breach to Plaintiffs and Class members in a timely manner.

(e) Sony did not act in a timely and reasonable way to cure these failures.

119. The breach of security and unauthorized access was reasonably foreseeable to Sony. Sony knew or should have known about the security defects before Plaintiffs' and Class members' sensitive Personal Information was stolen and should have taken active and reasonable steps to rectify such defects.

120. Sony knew or should have known that timely notification to the public would have allowed Plaintiffs and Class members the ability to take adequate measures to protect their Personal Information before it was used surreptitiously or improperly.

121. But for Sony's negligence, Plaintiffs' and Class members' Personal Information would not have been compromised.

122. As a proximate result, Plaintiffs and Class members have suffered injury-in-fact and lost money or property, including the theft of their valuable Personal Information.

COUNT V

Breach of Express Contract or, in the Alternative, Breach of Implied Contract

123. Plaintiffs hereby incorporate by reference each and every allegation set forth herein.

124. In exchange for purchasing PlayStation Equipment and various Network services, Plaintiffs and Class members entered into contracts whereby Sony agreed to provide uninterrupted Network service.

125. Customers' Personal Information is valuable property that was exchanged not only for Sony's Equipment and Network services, but also in exchange for Sony's promise to employ commercially reasonable methods to safeguard and secure the Personal Information that is exchanged. Indeed, as part of its PlayStation Privacy Policy, Sony expressly agreed to enact reasonable measures to protect the confidentiality, security, and integrity of its customers' Personal Information collected from its Customers and to have security measures in place to protect the loss, misuse, and alteration of its Customers' Personal Information. In exchange, Plaintiffs and Class

members agreed to purchase PlayStation 3 consoles, register for the PlayStation Network, and provide their Personal Information as required by Defendants.

126. In the alternative, an implied contract was created when Plaintiffs and Class members reasonably relied on Sony's express assurances of safety and security and registered for the Network service and transmitted sensitive Personal Information to Sony. Sony implicitly became obligated to reasonably safeguard that Personal Information.

127. By storing their Customers' Personal Information in unencrypted form and by failing to provide adequate or sufficient security to protect the PlayStation Network, Sony breached the agreement with its PlayStation Network Customers because Sony did not properly maintain the Personal Information of Plaintiffs and members of the Class.

128. As a result, Plaintiffs and Class members have suffered injury-in-fact and lost money or property, including the loss of their ability to access the Network and the theft of their valuable Personal Information.

COUNT VI

Breach of Fiduciary Duty

129. Plaintiffs hereby incorporate by reference each and every allegation set forth herein.

130. A fiduciary duty was created when the Plaintiffs and the Class members transferred their sensitive financial information to Sony, including credit card numbers, expiration dates, security codes, billing address and passwords in reasonable reliance on Sony's express assurances of maintaining the safety and security of Customers' Personal Information.

131. Sony did not act in the best interests of the Plaintiffs and Class members and thus breached its fiduciary duty by:

(a) Failing to take commercially reasonable measures to ensure the security of its Network, thus allowing for unauthorized access of Plaintiffs' and Class members' financial information;

(b) Failing to have in place commercially reasonable measures to timely detect and rectify a breach to its security; and

(c) Failing to notify the public of a breach to its security in a timely manner.

132. Instead, Sony acted in its own best interest to save money and protect its own confidential proprietary information, at the expense of Plaintiffs and members of the Class. It fired a significant portion of its workforce and used out-of-date security technology, or no technology at all, to safeguard Plaintiffs' and Class members' Personal Information.

133. As a direct and proximate result of Sony's breach, Plaintiffs and members of the Class have suffered injury-in-fact and lost money or property, including the theft of the valuable Personal Information.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class, pray for judgment as follows:

A. For an order certifying the Class and appointing Plaintiffs and their counsel to represent the Class;

B. Declaring that this action may be maintained as a Class action;

C. For an order enjoining Defendants from engaging in the unlawful, unfair, and fraudulent business practices and other legal violations alleged herein;

D. Actual damages in the amount of money paid for Equipment and the Network;

E. For an order requiring Defendants to make appropriate restitution to Class members;

F. For an order requiring Defendants to provide appropriate credit monitoring services to Class members;

G. For an order granting exemplary damages should the Court find that the Defendants acted in willful or reckless disregard of the law;

H. For an order awarding Plaintiffs and Class members pre-judgment and post-judgment interest;

I. For an order awarding Plaintiffs and Class members reasonable attorneys' fees and costs of suit, including expert witness fees; and

J. For such other relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all issues so triable as a matter of right.

DATED: June 20, 2011

ROBBINS GELLER RUDMAN
& DOWD LLP
RACHEL L. JENSEN

s/Rachel L. Jensen
RACHEL L. JENSEN

655 West Broadway, Suite 1900
San Diego, CA 92101
Telephone: 619/231-1058
619/231-7423 (fax)

ROBBINS GELLER RUDMAN
& DOWD LLP
PAUL J. GELLER
STUART A. DAVIDSON
MARK DEARMAN
120 E. Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)

LABATON SUCHAROW LLP
CHRISTOPHER J. KELLER
HOLLIS L. SALZMAN
KELLIE LERNER
CAROL C. VILLEGAS
140 Broadway
New York, NY 10005
Telephone: 212/907-0700
212/818-0477 (fax)

WHATLEY DRAKE & KALLAS
JOE R. WHATLEY, JR.
PATRICK J. SHEEHAN
SHUJAH A. AWAN
1540 Broadway, 37th Floor
New York, NY 10036
Telephone: 212/447-7070
212/447-7077 (fax)

Attorneys for Plaintiffs

S:\CptDraft\Consumer\Cpt Sony_SDCA.doc

JS 44 (Rev. 12/07)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON THE REVERSE OF THE FORM.)

I. (a) PLAINTIFFS

FELIX CORTORREAL, JACQUES DAOUD JR. and JIMMY CORTORREAL, on Behalf of Themselves and All Others Similarly Situated

(b) County of Residence of First Listed Plaintiff Nassau County, NY
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorney's (Firm Name, Address, and Telephone Number)
Rachel L. Jensen, Robbins Geller Rudman & Dowd LLP
655 W. Broadway, Ste. 1900, San Diego, CA 92101 619/231-1058

DEFENDANTS

SONY CORPORATION OF AMERICA, INC., SONY COMPUTER ENTERTAINMENT OF AMERICA, LLC, SONY PICTURES ENTERTAINMENT, INC., and SONY NETWORK ENTERTAINMENT INTERNATIONAL, LLC,
County of Residence of First Listed Defendant
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE LAND INVOLVED.

Attorneys (If Known)

'11CV1369 L NLS

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
- ☒ 3 Federal Question (U.S. Government Not a Party)
- ☐ 2 U.S. Government Defendant
- ☒ 4 ~~Diversity~~ yeb (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☐ 1	☒ 1 yeb	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☒ 2 yeb	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☐ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT (Place an "X" in One Box Only)

CONTRACT	TORTS		FORFEITURE/PENALTY	BANKRUPTCY	OTHER STATUTES
☐ 110 Insurance	PERSONAL INJURY	PERSONAL INJURY	☐ 610 Agriculture	☐ 422 Appeal 28 USC 158	☐ 400 State Reapportionment
☐ 120 Marine	☐ 310 Airplane	☐ 362 Personal Injury - Med. Malpractice	☐ 620 Other Food & Drug	☐ 423 Withdrawal 28 USC 157	☐ 410 Antitrust
☐ 130 Miller Act	☐ 315 Airplane Product Liability	☐ 365 Personal Injury - Product Liability	☐ 625 Drug Related Seizure of Property 21 USC 881	PROPERTY RIGHTS	☐ 430 Banks and Banking
☐ 140 Negotiable Instrument	☐ 320 Assault, Libel & Slander	☐ 368 Asbestos Personal Injury Product Liability	☐ 630 Liquor Laws	☐ 820 Copyrights	☐ 450 Commerce
☐ 150 Recovery of Overpayment & Enforcement of Judgment	☐ 330 Federal Employers' Liability	PERSONAL PROPERTY	☐ 640 R.R. & Truck	☐ 830 Patent	☐ 460 Deportation
☐ 151 Medicare Act	☐ 340 Marine	☐ 370 Other Fraud	☐ 650 Airline Regs.	☐ 840 Trademark	☐ 470 Racketeer Influenced and Corrupt Organizations
☐ 152 Recovery of Defaulted Student Loans (Excl. Veterans)	☐ 345 Marine Product Liability	☐ 371 Truth in Lending	☐ 660 Occupational Safety/Health	SOCIAL SECURITY	☐ 480 Consumer Credit
☐ 153 Recovery of Overpayment of Veteran's Benefits	☐ 350 Motor Vehicle	☐ 380 Other Personal Property Damage	☐ 690 Other	☐ 861 HIA (1395ff)	☐ 490 Cable/Sat TV
☐ 160 Stockholders' Suits	☐ 355 Motor Vehicle Product Liability	☐ 385 Property Damage Product Liability	LABOR	☐ 862 Black Lung (923)	☐ 810 Selective Service
☐ 190 Other Contract	☐ 360 Other Personal Injury		☐ 710 Fair Labor Standards Act	☐ 863 DIWC/DIWW (405(g))	☐ 850 Securities/Commodities/ Exchange
☐ 195 Contract Product Liability			☐ 720 Labor/Mgmt. Relations	☐ 864 SSID Title XVI	☐ 875 Customer Challenge 12 USC 3410
☐ 196 Franchise			☐ 730 Labor/Mgmt.Reporting & Disclosure Act	☐ 865 RSI (405(g))	☒ 890 Other Statutory Actions
REAL PROPERTY	CIVIL RIGHTS	PRISONER PETITIONS	☐ 740 Railway Labor Act	FEDERAL TAX SUITS	☐ 891 Agricultural Acts
☐ 210 Land Condemnation	☐ 441 Voting	☐ 510 Motions to Vacate Sentence	☐ 790 Other Labor Litigation	☐ 870 Taxes (U.S. Plaintiff or Defendant)	☐ 892 Economic Stabilization Act
☐ 220 Foreclosure	☐ 442 Employment	Habeas Corpus:	☐ 791 Empl. Ret. Inc. Security Act	☐ 871 IRS—Third Party 26 USC 7609	☐ 893 Environmental Matters
☐ 230 Rent Lease & Ejectment	☐ 443 Housing/ Accommodations	☐ 530 General	IMMIGRATION		☐ 894 Energy Allocation Act
☐ 240 Torts to Land	☐ 444 Welfare	☐ 535 Death Penalty	☐ 462 Naturalization Application		☐ 895 Freedom of Information Act
☐ 245 Tort Product Liability	☐ 445 Amer. w/Disabilities - Employment	☐ 540 Mandamus & Other	☐ 463 Habeas Corpus - Alien Detainee		☐ 900Appeal of Fee Determination Under Equal Access to Justice
☐ 290 All Other Real Property	☐ 446 Amer. w/Disabilities - Other	☐ 550 Civil Rights	☐ 465 Other Immigration Actions		☐ 950 Constitutionality of State Statutes
	☐ 440 Other Civil Rights	☐ 555 Prison Condition			

V. ORIGIN (Place an "X" in One Box Only)

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from another district (specify) ☐ 6 Multidistrict Litigation ☐ 7 Appeal to District Judge from Magistrate Judgment

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
Class Action Fairness Act of 2005, 28 U.S.C. §§1332(d), 1453, and 1711–1715 28:1331 yeb

Brief description of cause:
Complaint for Violation of California's Consumer Legal Remedies Act and Unfair Competition Law

VII. REQUESTED IN COMPLAINT:

☑ CHECK IF THIS IS A CLASS ACTION UNDER F.R.C.P. 23 DEMAND $ CHECK YES only if demanded in complaint:
JURY DEMAND: ☑ Yes ☐ No

VIII. RELATED CASE(S) IF ANY (See instructions): JUDGE Judge Anthony J. Battaglia DOCKET NUMBER 3:2011-cv-01001

DATE 06/20/2011

SIGNATURE OF ATTORNEY OF RECORD s/ Rachel L. Jensen

FOR OFFICE USE ONLY

RECEIPT # AMOUNT APPLYING IFP JUDGE MAG. JUDGE

JS 44 Reverse (Rev. 12/07)

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I. (a) **Plaintiffs-Defendants.** Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. **Jurisdiction.** The basis of jurisdiction is set forth under Rule 8(a), F.R.C.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.

United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.

United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.

Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.

Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below; federal question actions take precedence over diversity cases.)

III. **Residence (citizenship) of Principal Parties.** This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. **Nature of Suit.** Place an "X" in the appropriate box. If the nature of suit cannot be determined, be sure the cause of action, in Section VI below, is sufficient to enable the deputy clerk or the statistical clerks in the Administrative Office to determine the nature of suit. If the cause fits more than one nature of suit, select the most definitive.

V. **Origin.** Place an "X" in one of the seven boxes.

Original Proceedings. (1) Cases which originate in the United States district courts.

Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441. When the petition for removal is granted, check this box.

Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.

Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.

Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.

Multidistrict Litigation. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407. When this box is checked, do not check (5) above.

Appeal to District Judge from Magistrate Judgment. (7) Check this box for an appeal from a magistrate judge's decision.

VI. **Cause of Action.** Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553
Brief Description: Unauthorized reception of cable service

VII. **Requested in Complaint.** Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.

Demand. In this space enter the dollar amount (in thousands of dollars) being demanded or indicate other demand such as a preliminary injunction.

Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. **Related Cases.** This section of the JS 44 is used to reference related pending cases if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.